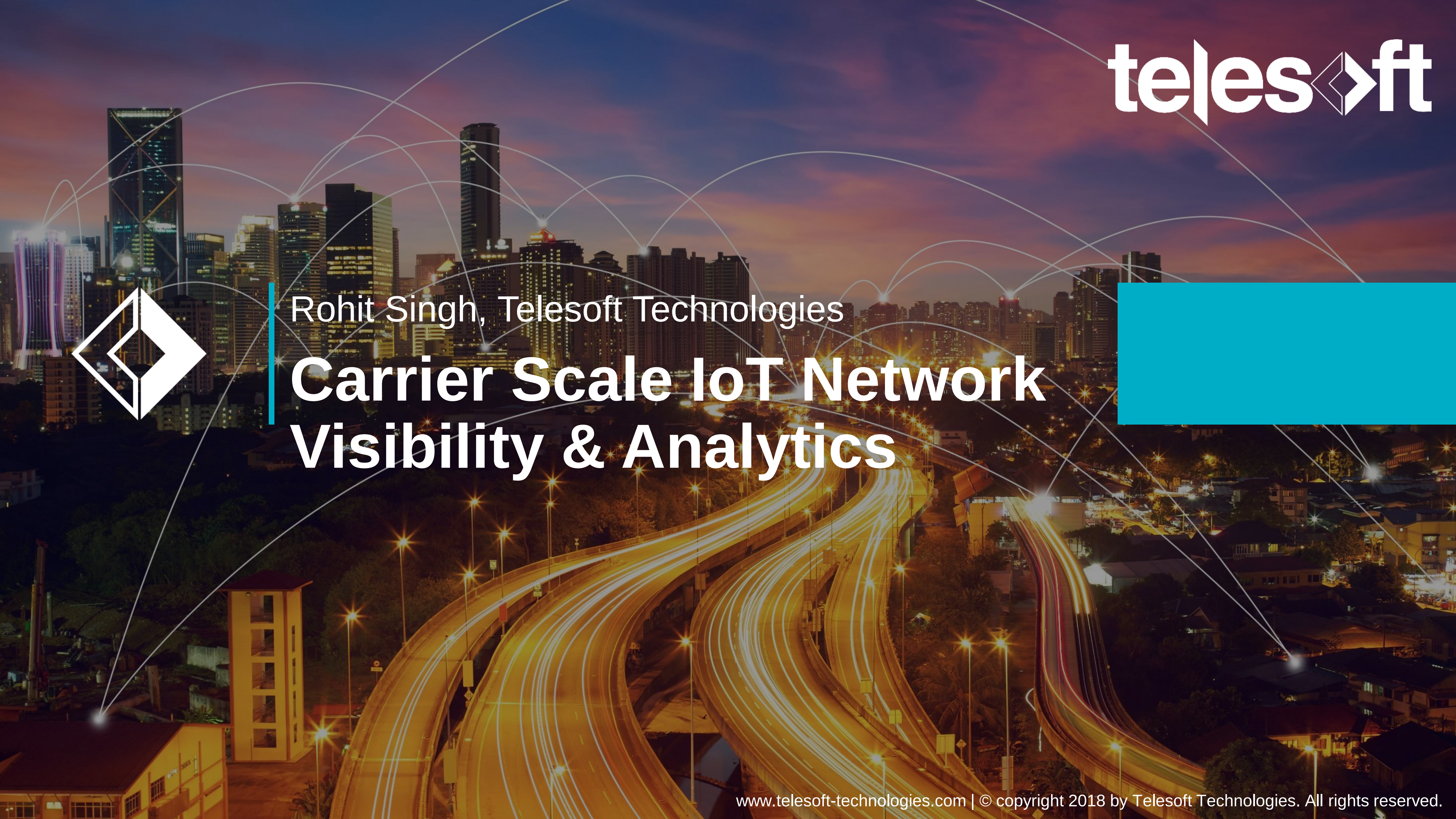


Rohit Singh, Telesoft Technologies

Carrier Scale IoT Network Visibility & Analytics

1
Introduction – Situation Analysis

- By 2020, Gartner® predicts, the Internet of Things will be made up of 26 billion “units.”
- Bain forecasts that the B2B IoT market will be worth $300B yearly by 2020.
- Embedded sensors are used to collect data from around the world. The IoT sensor market alone is expected to be worth a staggering $27 billion by 2022.
- IoT services will be strictly regulated, and security and privacy will be a primary future concern

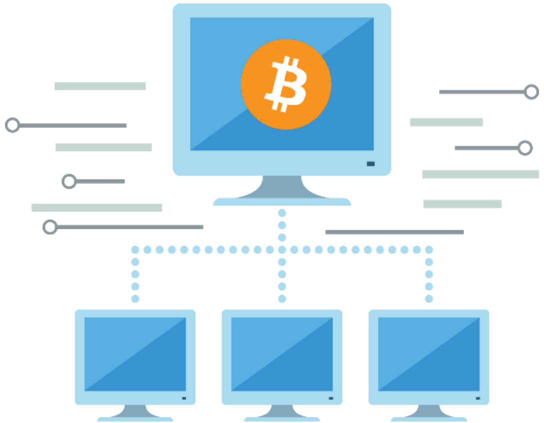
IoT Network Transformation

- IoT devices can be sourced from numerous unregulated manufacturers.
- The race is on to deliver functionality quickly. Cyber security is often a secondary concern.
- Until equipment build standards catch up with cyber security requirements the only protection is to monitor, analyse and detect anomalous behaviour and misuse of IoT devices.

telesoft

3
Types of attacks facing defenders

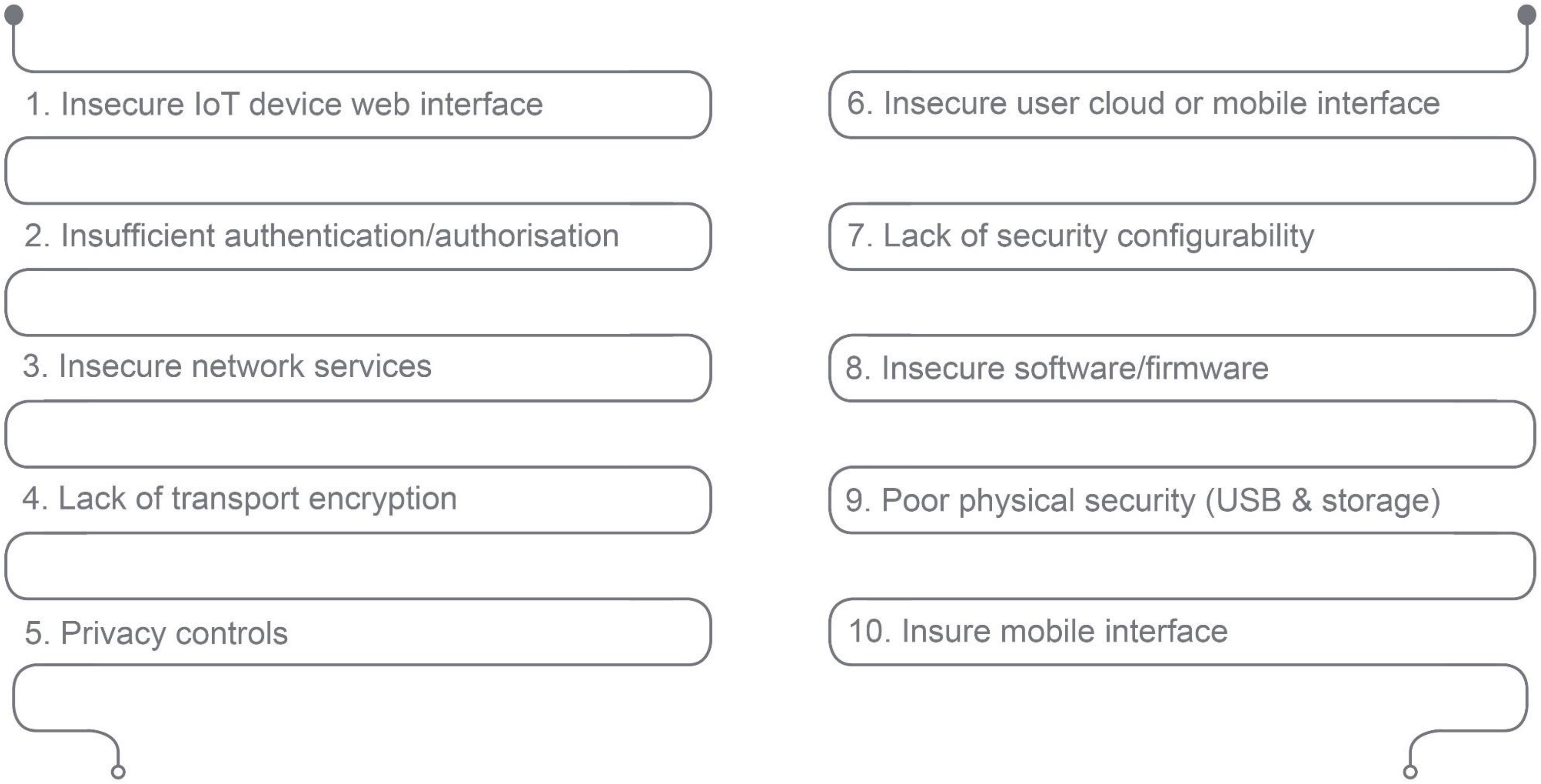
Unauthorised access and manipulation (e.g. cryptojacking & fraud)



Unauthorised control (e.g. Botnet/Zombie & disruption to device operation)

Data theft, collection and disclosure of unnecessary personal information

Common IoT Security Vulnerabilities for Service Providers



1. Insecure IoT device web interface
2. Insufficient authentication/authorisation
3. Insecure network services
4. Lack of transport encryption
5. Privacy controls
6. Insecure user cloud or mobile interface
7. Lack of security configurability
8. Insecure software/firmware
9. Poor physical security (USB & storage)
10. Insure mobile interface

The threat to IoT Infrastructure and CNI

- Attacks can have a direct effect across mass infrastructure:
  - Failure or disruption of transport systems, rail, air, road
  - Disruption to food supplies
  - Disruption of energy distribution
- Attack impact:
  - Minor inconveniences to an individual, e.g. interrupting physical access to a building or operation of in building smart system
  - Serious impact to a group, e.g. impact to distributed medical and critical life support devices.

5

Device Identification

- IoT devices that connect over 3G/4G mobile are often bulk provisioned using eSIM
- Connect through mobile NAT to cloud based applications

Unless there is sufficient control and monitoring

- 3G/4G IoT devices can be reprogrammed to access the network for unauthorised fraudulent services or initiate attacks / Botnet
- Attackers can hide their identity
- Infected IoT device cannot be identified
- Service is disrupted
- Damage to operators revenue and reputation

Telesoft in Carrier Scale Cyber Security

Telesoft's cyber products enable IoT connectivity providers to protect against attacks and maintain operation.

Anomalous Behaviour Discovery

Monitoring and detection devices that look for known threats and identify unusual and unexpected behaviour using :

- Meta-data
- Threat Intelligence
- Signatures
- Anomaly Detection algorithms

.

3G/4G /NB-IoT Device Identity

Monitoring and detection devices that enabling accurate device identity by correlating IP address to eSIM identity (IMSI/IMEI)

IP NAT Address Correlation

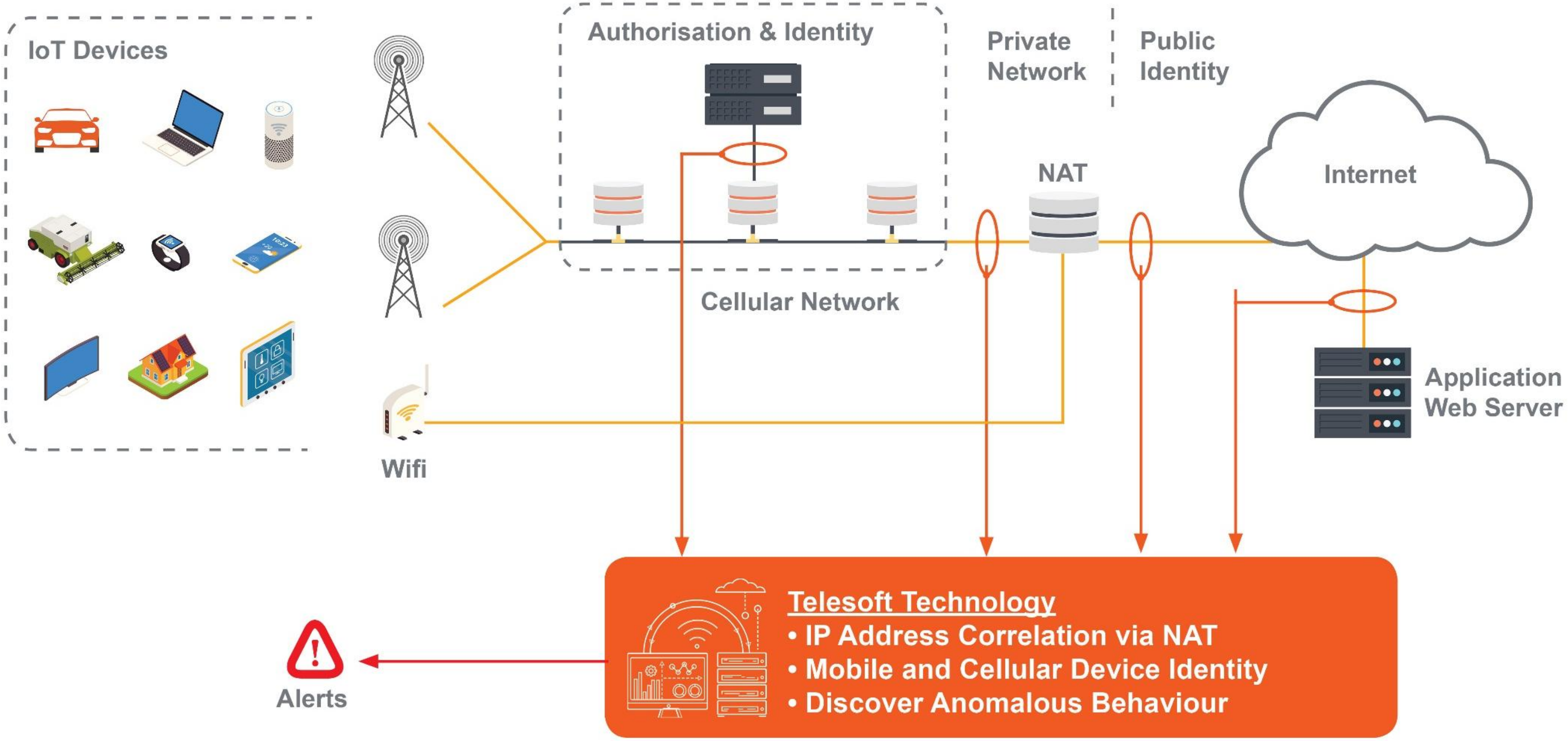
IoT devices often connect back through large scale address correlation (NAT) to cloud based applications.

The device may have a dynamically assigned and changing IP address, making identification of a specific device impossible.

Telesoft provides NAT correlation capability, meaning that anomalous behaviour and attack can be diagnosed to a single IoT device.

telesoft

7 Telesoft Infrastructure Integration



Telesoft Technology

- IP Address Correlation via NAT
- Mobile and Cellular Device Identity
- Discover Anomalous Behaviour

Summary

- IoT is…
  - Always on, always available, mobile connected
  - Attractive target for state activist, hackers
  - CNI, Power, Transport, Food, Medical, …

- Unless there is sufficient control and monitoring

  - Attackers can hide their identity.
  - 3G/4G IoT devices can be reprogrammed to access the network for unauthorised fraudulent services or initiate attacks / Botnet
  - Inability to identify infected IoT device

Thank You!